KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

Implementing Smart Privacy

Addressing Privacy Concerns in the California Smart Grid

Presentation to the California Public Utilities Commission

Jennifer M. Urban, Attorney
Director, Samuelson Law, Technology & Public Policy Clinic, UC-Berkeley
On behalf of CDT

October 25, 2010

Implementing Privacy Protections for Smart Grid Deployment

The CPUC must consider 4 key factors:

1. **The change in *amount* and *kind* of data flowing via Smart Grid technologies**
   - **Highly granular usage data that is revealing of intimate activities**
   - **Entirely new forms of revealing data, e.g., identifiable appliance IDs**
2. **The fact that data is/will be flowing through a new, complex ecosystem of providers**
3. **That the existing patchwork of laws and regulations applies only partially or imperfectly in the Smart Grid environment**
   - **Including the severe limitations of the obsolete notice-and-choice regime**
4. **The need to provide a balanced, flexible, comprehensive, and generalizable solution that allows for innovation and data flow, but protects customers' highly sensitive data**

These factors are best met by working from the full set of Fair Information Practice principles, as recognized by the Commission and many of the parties

Managing the Existing Legal Patchwork

- Overall, the existing welter of law and regulation creates a complicated, confusing, and inadequate patchwork
- While existing laws may apply adequately to certain information, to certain limited situations, or to certain entities, there are critical "gaps" in the existing regime
  - Cal. Pub. Util. Code 394.4 imposes a notice-and-consent rule
  - SB 1476, the newest update and the first to attend to the Smart Grid, addresses limited aspects of privacy
  - Policies need updating
  - Etc.
- Some useful approaches
  - Confidentiality and affirmative customer consent for various utility activities and programs (e.g., ESPs and affiliates)
  - Some use of contractual regimes

Gaps in privacy policies

"There are essentially no defenders anymore of the pure notice and choice model. ... It's no longer adequate." Daniel J. Weitzner, NTIA, US Dept of Commerce, New York Times, Feb 28, 2010.

Traditional methods may have been adequate in the past, but no longer fully protect customers

- **Need for privacy policies that cover *energy data or services* rather than website activity (but see PG&E's policy)**
- **Need for clear definitions, descriptions of use, and purposes**
- **Need for clarity about which parties might receive and use data**
- **Need for usable, granular controls over customer data**
- **Need for better information about data minimization, remedial options, etc.**

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Proposals

"Operationalizing" the FIPs for the Smart Grid environment:

1. **Create a comprehensive, general framework that can be understood and implemented by the Commission, Smart Grid entities, and customers**
2. **That draws from existing law and best practices**
3. **That fills gaps and updates privacy requirements for the Smart Grid ecosystem**
4. **That takes into account different relationships and data flows**

See Appendix A to CDT/EFF Opening Comment

We have received helpful input from PG&E, DRA and TURN

CDT Appendix A
CDT/PG&E Discussion Draft

1. DEFINITIONS

(a) **Covered Entity.** A "covered entity" is (1) any electrical service provider, electrical corporation, gas corporation or community choice aggregator, or (2) any third party that collects, stores, uses, or discloses covered information [relating to ___ or more households or residences*].

(b) **Covered Information.** "Covered information" is [any energy usage information concerning an individual, family, household, or residence, except that covered information does not include information from which identifying information has been removed such that it cannot reasonably be identified or re-identified with an individual, family, household, or residence][electrical or gas consumption data that includes the name, account number, or residence of the customer, or from which the name, account number or residence of the customer may be derived].

(c) **Primary Purposes.** The "primary purposes" for the collection, storage, use or disclosure of covered information are to—

(1) provide or bill for electrical power or natural gas,

(2) fulfill other operational needs of the electrical or natural gas system or grid, and

(3) provide services as required by state or federal law or required [or authorized] by an order of the Commission, or

(4) implement demand response, energy management, [or] energy efficiency[, or other utility] programs operated by, or on behalf of and under contract with, an electrical or gas corporation.

(d) **Secondary Purpose.** "Secondary purpose" means any purpose that is not a primary purpose.

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

*Comment: Some further thought needs to be given to the interplay between this threshold and the rules for legal process; we are concerned about unregulated governmental access to energy usage information from landlords of smaller apartment buildings.

CDT Appendix A
CDT/PG&E Discussion Draft

2. **TRANSPARENCY (NOTICE)**

(a) **Generally.** Covered entities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the collection, storage, use, and disclosure of covered information.

(b) **When Provided.** Covered entities shall provide notice in their first paper correspondence with the customer, if any, and shall provide conspicuous posting of the notice or link to the notice on the home page of their website.

(c) **Form.** The notice shall be labeled "Privacy Policy: Notice of Collection, Storage, Use and Disclosure of Energy Usage Information" and shall—

(1) be written in easily understandable language,

(2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice shall state clearly—

(1) the identity of the covered entity,

(2) the effective date of the notice,

(3) the covered entity's process for altering the notice, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and

(4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

CDT Appendix A
CDT/PG&E Discussion Draft

3. PURPOSE SPECIFICATION The notice required under section 2 shall provide—

(a) an explicit description of—

(1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the [reasonably] [specific] purposes for which it will be collected, stored, used, or disclosed, and

(2) each category of covered information that is disclosed to third parties [for a secondary purpose, or for a primary purpose under which the third party is providing services directly to customers], and, for each such category, (i) the purposes for which it is disclosed, and (ii) the identities of the third parties to which it is disclosed~~, and (iii) the value of the disclosure to the customer~~;

(b) the periods of time that covered information is retained by the covered entity;

(c) a description of ~~the choices available to customers and the means by which they may exercise those choices, including the means by which they may~~ —

(1) the means by which customers may view, inquire about, or dispute their covered information, and

(2) the means[, if any,] by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.~~; and~~

~~(d) the consequences to the customer, if any, of refusing consent to the covered entity, in whole or in part, regarding the collection, storage, use, or distribution of covered information.~~

CDT Appendix A
CDT/PG&E Discussion Draft

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

(a) **Access.** Covered entities shall provide to customers upon request convenient and secure access to their covered information—

(1) in an easily readable format [that is at a level of detail sufficient for the customer to utilize reasonably available energy management or energy efficiency products, but in no event] at a level [no] less detailed than that at which the covered entity discloses the data to third parties [for demand response, energy management or energy efficiency purposes].

(2) The Commission shall, by subsequent rule, prescribe what is a reasonable time for responding to customer requests for access.

(b) **Control.** Covered entities shall provide customers with convenient mechanisms for—

(1) granting and revoking authorization for secondary uses of ~~their~~ covered information,

(2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and

(3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

Continued on next slide…

CDT Appendix A
CDT/PG&E Discussion Draft

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL) ***Continued from last slide…***

(c) **Disclosure Pursuant to Legal Process.**

(1) Except as otherwise provided in this rule or expressly authorized by state or federal law or by order of the Commission, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law.

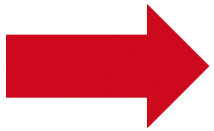
(2) Unless otherwise prohibited by court order or law or by order of the Commission, a covered entity, upon receipt of a demand for disclosure of covered information pursuant to legal process, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.

(3) Nothing in this rule prevents a person or entity seeking ~~energy usage~~ covered information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, written and specific to the purpose and to the person or entity seeking the information.

(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.

(6) On an annual basis, covered entities shall report to the Commission the number of times that customer data has been sought pursuant to legal process without customer consent, and for each such instance, whether it was a civil or criminal case, whether the covered entity complied with the request as initially presented or as modified in form or scope, and how many customers' records were disclosed. The ~~Commission should~~covered entity shall make such reports publicly available without identifying the affected customers, unless making such reports public is prohibited by state or federal law or by order of the Commission.



CDT Appendix A
CDT/PG&E Discussion Draft

5. DATA MINIMIZATION [GUIDELINE]

(a) **Generally.** Covered entities [shall][should] collect, store, use, and disclose only as much covered information as is [reasonably] necessary to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(b) **Data Retention.** Covered entities [shall][should] maintain covered information only for as long as [reasonably] necessary to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(c) **Data Disclosure.** Covered entities [shall] [should] not disclose to any third party more covered information than is [reasonably] necessary to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

CDT Appendix A
CDT/PG&E Discussion Draft

6. USE AND DISCLOSURE LIMITATION

(a) **Generally.** Covered information shall be used solely for the purposes specified by the covered entity in accordance with section 3.

(b) **Primary Purposes.** A ~~gas or electric corporation~~ covered entity may use covered information for primary purposes without customer consent.

(c) **Disclosures to Third Parties [to Carry Out a Primary Purpose].**

[(1) Initial Disclosure from a Utility.] A [gas or electrical corporation, electric service provider or community choice aggregator] [covered entity] may disclose covered information to a third party without customer consent [for a primary purpose] [when the third party is performing a primary purpose on behalf of a gas or electrical corporation, electric service provider or community choice aggregator][covered entity], provided that the [gas or electrical corporation, electric service provider or community choice aggregator] [covered entity] shall, by contract, require the third party [to commit, through a published privacy notice] to collect, store, use, and disclose covered information under policies and practices no less protective than those under which the [gas or electrical corporation, electric service provider or community choice aggregator] [covered entity] itself operates [in compliance with [as required under] this rule] [and, if the information is being disclosed for demand response, energy management or energy efficiency purposes, the gas or electric corporation, electric service provider or community choice aggregator permits customers to opt-out of such disclosure].

Continued on next slide…

CDT Appendix A
CDT/PG&E Discussion Draft

6. USE AND DISCLOSURE LIMITATION ***Continued from last slide…***

[(2) Onward Disclosures. Any entity that receives covered information derived initially from a gas or electrical corporation, electric service provider or community choice aggregator may disclose such covered information to another entity without customer consent for a primary purpose, provided that the entity disclosing the covered information shall, by contract, require the entity receiving the covered information to use the covered information only for such primary purpose and to commit, through a published privacy notice to store, use, and disclose the covered information under policies and practices no less protective than those under which the gas or electrical corporation, electric service provider or community choice aggregator from which the covered information was initially derived itself operates [in compliance with this rule].]

[(3) Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances. When an entity discloses covered information to any other entity under this subsection 6(c), it shall specify by contract that it shall be considered a material breach if the receiving entity engages in a pattern or practice of storing, using or disclosing the covered information in violation of the receiving entity's commitment to handle the covered information under policies no less protective than those under which the gas or electrical corporation, electric service provider or community choice aggregator from which the covered information was initially derived itself operates [in compliance with this rule]. If an entity disclosing covered information finds that an entity to which it disclosed covered information is engaged in a pattern or practice of storing, using or disclosing covered information in violation of the receiving entity's privacy and data security commitments related to handling covered information, the disclosing entity shall cease disclosing covered information to such receiving entity.]

Continued on next slide…

CDT Appendix A
CDT/PG&E Discussion Draft

6. USE AND DISCLOSURE LIMITATION ***Continued from last slide…***

(d) **Secondary Purposes**. No covered entity shall use or disclose covered information for any secondary purpose without obtaining the customer's prior, express, written authorization for each such purpose, provided that authorization is not required when information is—

(1) provided to a law enforcement agency in response to lawful process;

(2) [required][authorized] by the Commission pursuant to its jurisdiction and control ~~over electric and gas corporations~~.

(e) **Customer Authorization.**

(1) **Authorization.** Separate authorization by each customer must be obtained for each secondary purpose.

(2) **Revocation.** Customers have the right to revoke, at any time, any previously granted authorization.

[(3) **Expiration.** Customer consent shall be deemed to expire after two years, after which time customers will need to reauthorize any secondary purposes.]

(f) **Parity.** Covered entities shall permit customers to cancel authorization for any secondary ~~use~~purpose of their covered information by the same mechanism initially used to grant authorization.

CDT Appendix A
CDT/PG&E Discussion Draft

7. DATA QUALITY AND INTEGRITY

[Covered entities shall ensure that covered information they collect, store, use, and disclose is reasonably accurate and complete.]

8. DATA SECURITY

(a) **Generally.** Covered entities shall implement ~~appropriate~~reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

[(b) **Breach.** Covered entities shall disclose any breach in accordance with section 1798.82 of the Information Practices Act. In addition, covered entities shall notify the Commission of breaches of covered information.]

CDT Appendix A
CDT/PG&E Discussion Draft

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the ~~principles~~requirements herein, and must [file with] [make available to] the Commission [upon request or audit]—

(1) the privacy notices that they provide to customers,

(2) their internal privacy [and [data] security] policies,

(3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose, and

(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

[(b) **Redress.** Covered entities shall provide customers with mechanisms for ~~appropriate~~reasonable access to covered information, for correction of inaccurate covered information, and for redress in the event of a violation of these rules.]

(c) **Training**. Covered entities shall provide ~~appropriate~~reasonable training to all employees and contractors who use, store or process covered information.

(d) **Audits**. Covered entities shall conduct an independent audit of [[data] security] and privacy practices at least [once per year] to monitor compliance with its privacy [and [[data] security] commitments, and shall report the findings to the Commission.

(e) **Disclosures**. On an annual basis, covered entities shall disclose to the Commission—

(1) the number and identities of authorized third parties accessing ~~customer energy usage~~covered information,

[(2) the number of security breaches experienced by the electrical corporation or gas corporation, and

(3) the number and percentage of customers affected by breaches of covered information.]